

A portrait of Nils Biedermann, a man with dark hair, a mustache, and a goatee, wearing a dark suit jacket over a white shirt. The background is a dark blue gradient with a faint image of a space shuttle launching.

**Nils Biedermann**

# AI as the space race of the 21st century

The Danger of AI-driven Disinformation Campaigns for Foreign and Security Policy

## 3 Main Points

- Does AI pose a threat to security and foreign policy due to the possibility of disinformation campaigns against the backdrop of technological advantages other nations?



- The targeted dissemination of false information can influence the sentiment of the respective population or politicians themselves and can be part of hybrid warfare.
- It is therefore important not only to possess the sword, but also the shield. The shield must be a strong AI strategy for the EU in the context of defense.

### **About the Author**

Academic background in law (first state examination at the University of Cologne and a master's degree in Media Law and Media Economics at the University of Applied Science Cologne) and computer science (current master's degree program in Legal Informatics at the University Passau). Professional experience in the field of data protection law, cybersecurity, artificial intelligence compliance and development of new data-driven business models in the highly regulated telecommunication sector.

### **AI as the space race of the 21st century**

The proliferation of artificial intelligence (AI) beyond the private and public sectors into foreign and security policy marks a fundamental shift in international relations. The exponential growth in AI capabilities, from predictive analytics to autonomous systems, presents nations with both unprecedented strategic opportunities and formidable risks. The race for the most powerful AI could become the space race of the 21st century. While the United States currently maintains a leading role, the People's Republic of China has emerged as a colossal rival, driven by ambitious state-backed investments. Trapped between these two technological poles, the European Union (EU) must define and implement a cohesive strategy to secure its own interests. Against this backdrop, the following section outlines the dangers of AI in the field of disinformation for democracy and foreign policy, which make an AI strategy for the EU very important.

Historical example of disinformation in politics



Historically, the deliberate spread of misinformation has been a potent tool for triggering conflicts. A well-known example from the analogue era is the Ems [telegram](#), a manipulated diplomatic communication that was skilfully used by Prussian Chancellor Otto von Bismarck to incite the Franco-Prussian War of 1870–1871. This historical precedent highlights a core vulnerability that has been fundamentally exacerbated by the rise of artificial intelligence. If AI-driven technology on the opposing side becomes so advanced that it can deceive even government officials, it poses an existential threat to strategic stability and rational decision-making.

### The capabilities of AI in the field of disinformation and its dangers

In both conventional warfare and the provision of international aid, public support is a critical component of national strategy. Widespread domestic resistance can force a government to alter its foreign policy decisions, making public opinion a vital objective for both allies and adversaries. Especially before elections, it is paramount that the population cannot be manipulated by false information. The integration of artificial intelligence into security and defence strategies expands the scope of hybrid warfare. AI systems make it possible to conduct automated and targeted information. AI disinformation warfare in tandem with conventional military actions, which increasingly blurs the line between physical and cognitive dimensions of conflict. Three capabilities in this context make AI particularly dangerous: the creation, dissemination, and analysis and adaptation of content.

First, AI enables the generation of deceptively authentic information material like manipulated or completely generated videos and audio recordings. With these deepfakes, politicians can be deliberately discredited, false reports spread, or diplomatic relations sabotaged. The deception of governments themselves is also coming into focus. This can be dangerous, especially if the enemy country has a technological advantage in the development of artificial intelligence. With rapid technological progress, it is becoming increasingly difficult to distinguish manipulated videos, as the fluid image sequences suggest an authenticity that the public is not yet accustomed to due to its prolonged familiarity with image editing.



Second, AI can exponentially increase the reach of this disinformation. Automated content creation makes it possible to produce an enormous amount of slightly varied content in a very short time, giving the impression that the information comes from many independent sources. Researchers demonstrate that at least 400,000 bots interfered in the political discussion surrounding the 2016 US presidential election on platform X. The automated accounts produced an estimated 20 percent of all tweets related to the topic.

A third, particularly dangerous, application of AI is targeted amplification. AI algorithms can analyse social media to identify cognitive vulnerabilities in public opinion. They then deploy automated bots to disseminate disinformation to susceptible groups, exponentially increasing its reach. By operating within closed online communities, these bots can create the illusion of a majority consensus, such as in the comments section of a news article. This process is continuous and adaptive, with the AI constantly modifying its content and strategy in real-time to maximize engagement and viral potential across multiple platforms simultaneously.

Psychological effect and influence on the sentiment within the population

The targeted dissemination of false information can influence the sentiment of the respective population. It can generate approval or disapproval of the government's current actions. It can also influence attitudes toward other countries. For instance, the availability heuristic describes the human tendency to overestimate the likelihood of events that are easily recalled, which makes recent, or frequently repeated disinformation seem more credible. Additionally, confirmation bias leads people to favour information that confirms their existing beliefs, making them more likely to accept false narratives that align with their worldview.



This is often the first step toward conspiracy ideation, the tendency to attribute events to the malicious actions of powerful groups, even without evidence. One example of this phenomenon is the debate surrounding wind turbines. In this case, availability heuristics are local debates in which residents repeatedly hear about the negative aspects of wind turbines, such as noise pollution, shadow casting, or species protection issues. These repeated, concrete reports are easily accessible and lead people to overestimate the likelihood of these disadvantages, while the global benefits of renewable energies fade into the background. This creates confirmation bias. Those who already believe that climate protection measures are too expensive or ineffective will cite reports of birds dying from wind turbines as proof of the futility of the energy transition. Studies on the efficiency of wind energy are ignored. Ultimately, this leads to conspiracy theories. The opinion is elevated to the assumption that the “green energy lobby” is running a “corrupt business” with wind turbines through subsidies and political influence and is covering up the true ecological damage.

The rapid, viral dissemination of disinformation online makes it incredibly difficult to counter. Disinformation leverages cognitive biases to create in-group/out-group dynamics, ultimately contributing to a climate of political and social fragmentation. The goal is not just to spread a lie, but to engineer mass psychological shifts that weaken national cohesion and political stability. Experiments show that a 2-4 % bot participation of a communication network can be sufficient to tip over the opinion climate in two out of three cases.

## Conclusion

The integration of artificial intelligence into foreign and security policy represents a paradigm shift, fundamentally transforming the nature of modern conflict. The digital landscape is no longer merely a battlefield for ideas, but a domain where disinformation can be weaponized with unprecedented speed, scale, and psychological precision. Keeping pace with the ongoing development of artificial intelligence is particularly important here and needs a strong investment offensive. Only if you are at the same technological level as your opponent can you withstand an



attack on the truth. Also, an AI education initiatives to make the population resilient to disinformation or to train experts can be a part of the AI strategy. It is therefore important not only to possess the sword, but also the shield. The shield must be a strong AI strategy for the EU in the context of defence.